آموزش اولویت بندی درخواستهای Login به دومین کنترلرها به زبان ساده (نسخه PDF)

شاید تا به حال بر این باور بوده اید که در یک شبکه زمانیکه شما دو یا بیش از دو عدد Domain Controller راه اندازی می کنید درخواست ها بین این Domain Controller ها برای احراز هویت کلاینت ها و همچنین Logon به سیستم ها تقسیم می شود. این برداشت تا حدودی نـادرست است. ما می توانیم بر اساس نیاز خودمان سـرورهای Domain Controller را برای احراز هـویت و Logon کلاینت ها اولویت بندی کنیم و در واقع درخواست های مختلف را به سـرورهای مختلف ارسال کنیم و خودمان بصورت دستی برای کلاینت ها محدوده احزا هویت تعریف کنیم . اینکـار توسط دو پارامتر در رکوردهای SRV سرویس DNS به نامهای **Weight** و **Priority** تعریف می شود و شما با دستکاری این دو رکورد در LDAP SRV Record می توانید اولویت های خود را تغییر بدهید.

تصور کنید که در شـبکه ای قرار دارید که نرم افزارهای سـرورهای شـما بصورت جداگانه و کلاینت های شما هم بصورت جداگانه به Domain Controller درخواست احراز هویت می دهند و آنقدر سر Domain Controller شلوغ می شود که بعضا نمی تواند به درخواست های کلاینت ها پاسخ بدهد ، در چنین مواقعی شـما می توانید دو عدد Domain Controller در شبکه با weight و priority مختلف ایجاد کنید که یکی از آنها فقط درخواست های کلاینت ها را پاسخگویی کند و دیگری فقط و فقط درخواست های نرم افزارهای کاربردی سرورها را پاسخ بدهد.

کلاینت ها زمانیکه می خواهند به یک Domain Controller درخواست Login بدهند ابتدا درخواست خود را به DNS سرور ارسال می کنند ، DNS سـرور لیستی از Domain Controller هایی را که سـرویس Kerberos و LDAP ارائه می دهنـد را به کلاـینت ارسال می کنـد ، در این لیست دو پارامتر **weight** و **priority** نیز ارسال می شود که کلاینت بر اساس آنها تصمیم می گیرد که باید درخواست خود را به کدامیک از سرورهای مذکور ارسال کند به مثال زیر توجه کنید در این شـبکه سه عدد Domain Controller وجود دارد که درخواست کلاینت به شکل زیر پاسخ داده شده است :

```
_exmp1.tcp.tosinso.com IN SRV 10 50 389 server1.tosinso.com
_exmp1.tcp.tosinso.com IN SRV 10 50 389 server2.tosinso.com
_exmp1.tcp.tosinso.com IN SRV 10 50 389 server3.tosinso.com
```

در مثالی که در بالا مشاهده می کنید و نتیجه **Query** یک کلاینت از DNS سرور برای پیدا کردن Domain Controller مناسب برای Login به سیستم است عدد ۱۰ نمایانگر priority یا اولویت و عدد ۵۰ به عنوان weight یا بار در server۱.tosinso.com نشان داده شده اند. در مثال بالا کلاینت های شبکه همیشه برای احراز هویت از سرور server۱.tosinso.com استفاده خواهند کرد و تا زمانیکه این سرور در شبکه فعال باشد به سـراغ سرورهای دیگر نخواهند رفت. اگر می خواهید کلاینت های شما همیشه برای احراز هویت از سرور server۲.tosinso.com استفاده کنند بایستی مقدار عددی priority مربوط به سرور server۲.tosinso.com را در کنسول مدیریتی DNS تغییر بدهید.

کلاـینت ها در صورتیکه همه موارد از قبیل **weight** و **priority** برای همه سـرورها برابر باشد همیشه از سـرور اولی که در Query بازگشت داده می شـود برای احراز هـویت اسـتفاده می کننـد. کلاـینت هـا همیشه برای احراز هویت به دنبـال سـروری هسـتند که دارای priority پایینتری باشد. برای مثال اگر شما عدد priority مربوط به سرور server۲.tosinso.com را تغییر بدهید و از عدد ۱۰ به عدد ۶ تبدیل کنید. بعد از اعمـال تغییرات در SRV Record در DNS سـرور ، زمانیکه کلاینت از سـرور برای رکوردهای مورد نظر Domain Controller ها Query بگیرد اینبار پاسخ DNS سرور به شکل زیر خواهد بود و ترتیب معرفی سرورها تغییر خواهد کرد :

```
_exmp1.tcp.tosinso.com IN SRV 6 50 389 server2.tosinso.com
_exmp1.tcp.tosinso.com IN SRV 10 50 389 server1.tosinso.com
_exmp1.tcp.tosinso.com IN SRV 10 50 389 server3.tosinso.com
```

هر کلاینتی که به شبکه دومین ویندوزی ما Join می شود برای پیدا کردن Domain Controller مورد نظر خود برای Login کردن به اکتیودایرکتوری و پروتکل LDAP از یک Component به نام **DCLocator** که به عنوان یکی از اجزای سرویس **NETLOGON** وجود دارد استفاده می کند. همانطور که قبلا هم در پاراگراف های قبلی در این مقاله انجمن تخصصی فناوری اطلاعات ایران ذکر کردیم باید منطقی پشت این ماجرا باشد که بعد از درخواست کلاینت از DNS سرور **DCLocator** از کجا متوجه می شود که باید از کدام Domain Controller استفاده کند ؟ بر اساس تجربیات خودم (Unity) و همچنین جستجوهایی که در این خصوص انجام داده ام به این نتایج رسیده ام که عوامل زیر برای تعیین کردن سرور Login کلاینت ها بسیار مهم هستند :

۱. نسخه یا Version سیستم عامل سرور Domain Controller (سیستم عامل جدیدتر زودتر از سیستم عامل قدیمی جواب می دهد)
۲. واکنش سریعتر سرورها (معمولا سرورها با منابع بیشتر سخت افزاری سریعتر پاسخ می دهند)
۳. ترتیب رکورد هایی که از طریق DNS مشابه پاراگراف های قبلی بازگشت داده می شود (رکوردهای gc__ و ldap__)
۴. مقادیر priority و weight ای که برای رکوردهای SRV دامین کنترلرها تعریف می شود.

موارد متعدد و سناریوهای مختلفی وجود دارد که در آنها شما مجبور هستید که درخواست های LDAP ای که توسط سیستم های کلاینت ها ارسال می شوند را بین بیش از یک Domain Controller تقسیم کنید ، بصورت پیشفرض بر خلاف تصوراتی که می شود اکثر درخواست های کلاینت ها توسط یک Domain Controller انجام می شود ، از جمله این سناریوها که ما باید درخواست های LDAP را به سرورهای مختلف تقسیم کنیم به موارد زیر می توانیم اشاره کنیم :

۱. Domain Controller ای که دارای نقش PDC Emulator است بسیار پر کار شده است و کارایی Login و احراز هویت کاربران کم شده است
۲. بروز رسانی و یا مهاجرت سرورهای Domain Controller به یک سیستم عامل جدید باعث شده همه درخواست ها در سیستم عامل جدید پاسخگویی شوند
۳. می خواهید احراز هویت سرورها و سرویس های سازمان توسط یک Domain Controller اختصاصی انجام شود و نه توسط همان Domain Controller ای که همه سیستم های کلاینت ها از آن استفاده می کنند.

سرویس Netlogon از دو پارامتر برای کنترل کردن پاسخ های درخواست های LDAP به نام های **LdapSrvWeigth** و **LdapSrvPriority** استفاده می کند. بصورت پیشفرض هر DC یک priority با عدد صفر و یک weight با عدد ۱۰۰ دارد همانطور که در مثال اول همین مقاله مشاهده کردید. پارامتر weight باعث می شود که DC هایی که دارای priority یکسان هستند اما weight بالاتری دارند پاسخگو تر باشند. اما اگر پارامتر priority پیکربندی شود بر روی پارامتر weight اولویت خواهد داشت.Domain Controller هایی که دارای بالاترین نمره weight باشند و کمترین priority را داشته باشند بیشتر با آنها تماس برقرار می شود. برای اینکه این رفتار را بتوانیم تغییر بدهیم ، بایستی دو عدد کلید رجیستری در Domain controller های مورد نظرمان بصورت **REG__DWORD** در مسیر زیر به نامهای **LdapSrvWeight** و **LdapSrvPriority** ایجاد کنیم :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Netlogon\Parameters
```

عددی که می توانیم انتخاب کنیم برای هر یک از پارامترهای ایجاد شده می تواند بین ۰ تا ۶۵۵۳۵ باشد ، بعد از اعمال تغییرات بر روی Domain Controller مورد نظر سرویس Netlogon را یکبار Restart کنید و در کنسول DNS به SRV Record های مورد نظر مراجعه کنید و مطمئن شوید که تغییرات اعمال شده است ، تغییرات معمولا بلا فاصله ایجاد می شود ، برای مثال در جاییکه شما می خواهید دو عدد سرور همیشه پاسخگو باشند پیشنهاد می شود که weight سرور اول را ۵۰ و priority آن را ۱۰ قرار بدهید و برای سرور دوم عدد ۱۰۰ را برای weight و عدد ۱۰ را برای priority تعریف کنید و در نهایت برای سومین سرور که سرور بیکار ما خواهد بود عدد ۱۰۰ را برای priority و عدد ۰ را برای weight قرار بدهید . **ITPRO باشید**

نویسنده : محمد نصیری

منبع : جزیره سرویس های شبکه مایکروسافت وب سایت توسینسو

Mehran Eshghi

ممنون اسـتاد عزیز ، مقاله خیلی خوبی بود ، در شـبکه ما فارست با چندین دومین داریم.در یکی از دومین ها ۲عدد دومین کنترولر یه نام DC۱ و DC۲ که دومی نقش Additional رو بازی میکنه راه اندازی کردیم.با توجه به توضیحات شما دو سوال در ذهن من ایجاد شد

سوال اول: من میتونم الان بگم تمامی کلایتنها برای لاگ این کردن از Additional استفاده کنند و برای بقیه موارد ار دومین اصلی؟(چه برای کلاینت هایی که جوین هستند و چه برای اونهایی که تاره جوین میشند)مشکلی پیش نمیاد؟

سوال۲: گفته خودتون: "برای مثال در جاییکه شـما می خواهید دو عدد سرور همیشه پاسخگو باشند پیشنهاد می شود که weight سرور اول را ۵۰ و priority آن را ۱۰ قرار بدهید و برای سـرور دوم عدد ۱۰۰ را برای weight و عدد ۱۰ را برای priority تعریف کنید و در نهایت برای سومین سرور که سرور بیکار ما خواهد بود عدد ۱۰۰ را برای priority و عدد ۰ را برای weight قرار بدهید "*

شما در این مثال میگید سـرور سوم بیکاراست.اما این سرور در اولویت پاسخگویی قرار دارد با توجه به توضیحاتی که دادین،به نظر من در این سناریو اول سرور دوم پاسخ میده بعدا سرور سوم(چون وزن بالا با اولویت پایین در ارجعیته(ظبق گفته خودتون) و در آخر سرور اول به عنوان سرور بیکار ایفای نقش میکنه) ، ممنون میشم توضیح کاملتر بیان کنید؟

مطلب اصلی